4. What is ../../ used for in FI?

The `../../` pattern is often used in File Inclusion (FI) attacks as a **path traversal** technique. It allows attackers to navigate up directories to access files outside the intended directory.

Explanation of `../../`

- In file paths, `../` refers to the parent directory, and `../../` means going up two directories.
- By stacking `../`, an attacker can move further up the directory structure, escaping from the current folder to higher-level folders.

Example of Path Traversal in LFI

In a vulnerable application, the attacker might be able to control the path of an included file. For example, if the application's code looks like this:

```
<?php
  $file = $_GET['page'];
  include("pages/" . $file);
?>
```

If the attacker sends a request like `page=../../../../etc/passwd`, the application would attempt to include `/etc/passwd` by going up the directory hierarchy.

Goal of Path Traversal in FI Attacks

By using path traversal, attackers try to:

1. **Access Sensitive Files**: Access files like `/etc/passwd` (on Linux) or configuration files containing sensitive information.
2. **View Source Code**: Include files within the application's source code to study its structure, identify other vulnerabilities, or retrieve sensitive information.
3. **Exploit Further Vulnerabilities**: If they can include writable files, they may use this for further attacks, such as injecting code.

Mitigating Path Traversal in FI Attacks

To prevent this, use absolute paths, input validation, whitelisting, and other security measures mentioned above.